UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

DANIEL COZZA, individually and on behalf of all others similarly situated, Plaintiff, v. BANSLEY AND KIENER, L.L.P., Defendant.	Case No.: _____ **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Daniel Cozza ("Plaintiff"), individually and on behalf of the proposed Classes defined herein, alleges the following against Bansley and Kiener, L.L.P. ("B&K" or "Defendant") based upon personal knowledge, experience, information, and belief, including investigation conducted by their attorneys and review of public documents as to all other matters.

I. NATURE OF THE CASE

1. In a recent Executive Order, President Joe Biden reaffirmed that "[t]he United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy."[1] Among other things, the Order noted:

> The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (last accessed Dec. 21, 2021).

> should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.[2]

2. Plaintiff brings this class action case against Defendant for its failures to secure and safeguard the private and sensitive information it collected, maintained, stored, analyzed, and used to provide its services. That information includes, but is not limited to, personally identifiable information ("PII") such as full names and Social Security numbers of over 274,115 individuals,[3] and unsecured protected health information ("PHI") of approximately 70,941 individuals[4] (collectively, "Sensitive Information").

3. Armed with the Sensitive Information acquired in the Data Breach, data thieves are able to commit numerous crimes including opening new financial accounts in Class members' names, taking out loans in Class members' names, using Class members' names to obtain medical services, using Class members' information to obtain government benefits, filing fraudulent tax returns using Class members' information, obtaining driver's licenses in Class members' names but with another person's photograph, and giving false information to police during an arrest.

4. As a result of the Data Breach, Plaintiff and Class members have been exposed to a present and continuing risk of fraud and identity theft. Plaintiff and Class members must now and in the future closely monitor their financial accounts to guard against identity theft.

5. Plaintiff and Class members will also incur out-of-pocket costs for things such as paying for credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

---

[2] *Id.*

[3] Office of the Maine Attorney General, *Data Breach Notifications*, https://apps.web.maine.gov/online/aeviewer/ME/40/36b0a9a6-30c4-4942-9095-aaf86cfba741.shtml (Last accessed December 21, 2021.)

[4] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Dec. 21, 2021)

6. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Sensitive Information was accessed during the Data Breach.

7. Plaintiff and the Class seek remedies including damages, reimbursement of out-of-pocket costs, and equitable and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and identity protection services funded by Defendant.

II. PARTIES

8. Plaintiff Daniel Cozza is resident of the state of Missouri. Mr. Cozza received a Notice of Data Breach from Defendant dated November 24, 2021.

9. Defendant Bansley and Kiener, L.L.P. is an Illinois limited liability partnership. Defendant's principal place of business is located at 8745 West Higgins Road, Suite 200, Chicago, IL 60631. B&K is a full-service CPA and advisory firm, delivering accounting, tax, consulting, and assurance services to businesses of all sizes.

III. JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1331(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members, and at least some members have a different citizenship from Defendant.

11. This Court has personal jurisdiction over Defendant because B&K is an Illinois limited liability partnership and maintains its principal place of business in Chicago, Illinois; its nerve center, including its CEO, is in Illinois; it regularly conducts business in Illinois; and it has sufficient minimum contacts in Illinois. Defendant intentionally availed itself of this jurisdiction by providing services and by accepting and processing payments for those services within Illinois.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because B&K's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District. Further, venue is proper under 28 U.S.C. § 1391(b)(3) because Defendant is subject to personal jurisdiction in this District.

IV. FACTUAL ALLEGATIONS

A. Background

13. Defendant Bansley & Kiener, L.L.P is a full-service CPA and advisory firm based in Chicago, Illinois. It provides accounting, tax, consulting, and assurance services to businesses of all sizes, and conducts compliance engagements for benefit plans—including, but not limited to, health and pension plans. To provide these services, Defendant collects, maintains, stores, analyzes, and uses Sensitive Information belonging to Plaintiff and Class Members.

14. Because Defendant collects, maintains, stores, analyzes, and uses Sensitive Information, Defendant was and is legally required to protect the Sensitive Information in its possession from unauthorized access and acquisition.

15. However, Defendant failed to implement reasonable, adequate, and industry standard security measures on its IT network where it stored and maintained Sensitive Information, thus allowing an unauthorized party to access and steal Plaintiff's and other individuals' Sensitive Information. To make matters worse, Defendant failed to timely notify impacted individuals.

B. The Data Breach

16. Between August 20 and December 1, 2020, an unauthorized party (or parties) accessed and stole Sensitive Information belonging to Plaintiff and Class Members from Defendant's computer systems (the "Data Breach).[5]

[5] Office of the Maine Attorney General, *Data Breach Notifications*, *supra* note 3.

17. On or about December 10, 2020—three months after the unauthorized access began—Defendant identified an incident on its computer system containing the Sensitive Information belonging to Plaintiff and other impacted individuals ("Class Members").[6]

18. On May 24, 2021, Defendant realized data had been exfiltrated during the Data Breach.

19. Fifteen months after the Data Breach was discovered, Defendant publicly acknowledged the data security incident to state attorneys general in late November 2021.

20. Also on or about November 30, 2021—fifteen months after the Data Breach began, and eleven months after the Data Breach was discovered—Defendant began notifying affected individuals, including Plaintiff and Class Members, of the Data Breach.[7]

21. According to Defendant, the unauthorized party had access to its server containing Sensitive Information for three months before Defendant noticed the unauthorized access.[8]

22. Defendant failed explain why it took three months to notice and/or realized an unauthorized party had access to its network, or why it waited another fifteen months to begin notifying Plaintiff and Class Members of the Data Breach.

23. Plaintiff and Class Members had their Sensitive Information accessed and stolen by an unauthorized party due to Defendant's acts and omissions and its failure to properly protect the Sensitive Information it collected, maintained, analyzed, and used.

---

[6] *See* http://www.bk-cpa.com/data-security-incident-notice/ (last accessed Dec. 21, 2021).

[7] Office of the Maine Attorney General, *Data Breach Notifications*, *supra* note 3.

[8] Office of the Maine Attorney General, Copy of notice, https://apps.web.maine.gov/online/aeviewer/ME/40/36b0a9a6-30c4-4942-9095-aaf86cfba741/eebb91ba-baca-4b6d-a159-3a63996e166e/document.html (last accessed Dec. 21, 2021)

24. Defendant should have prevented this Data Breach. Data breaches are a well-known and well publicized problem, thus providing notice to Defendant that the Sensitive Information in its possession could be targeted by unauthorized parties, or "hackers." The Data Breach was the inevitable result of Defendant's inadequate approach and/or attention to data security and protection of the Sensitive Information it collects, maintains, analyzes, and uses to generate reports in the normal course of business.

25. Defendant disregarded the rights of Plaintiff and Class Members by recklessly, and/or negligently failing to implement industry standard security measures or otherwise take adequate and reasonable measures to ensure protection of its data systems; by failing to disclose the material fact that Defendant did not have adequate computer security systems and practices to safeguard the Sensitive Information it collected, maintained, analyzed, and used; and by failing to take available steps to prevent and stop the breach from ever happening; and failing to monitor and detect the breach in a timely manner.

26. As a result of the Data Breach, Plaintiff's and Class Members' Sensitive Information was exposed to and acquired by unauthorized parties—criminals—for misuse, identity theft, and other fraudulent activities. The exfiltrated Sensitive Information is likely already being used by unauthorized part(ies) to commit identity theft, including applying for credit cards, taking out loans, and leasing equipment. The injuries suffered, or likely to be suffered by Plaintiff and Class Members as a direct result of Defendant's Data Breach include, but are not limited to:

a. Theft of their personal and financial information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. Damages arising from the inability to use their own Sensitive Information;

d. Restricted or inability to access their account funds, including the costs and fees associated with inability and/or restrictions on obtaining funds from their accounts or limits on the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

e. Costs, including lost opportunity costs, associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;

f. The imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Sensitive Information being placed in the hands of criminals;

g. The continued risk to Plaintiff's and Class Members' Sensitive Information in Defendant's possession, which remains accessible to Defendant and subject to further breaches so long as Defendant fails to undertake appropriate, reasonable, industry standard, and commercially available measures to protect the Sensitive Information in its possession; and

h. The loss of Plaintiff's and Class Members' privacy.

27. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement and/or maintain adequate data security measures for the Sensitive Information it collects, maintains, analyzes, and uses in the normal course of business.

28. Additionally, Plaintiff and Class Members retain a significant interest in ensuring their Sensitive Information, which—despite being accessed and acquired by an unauthorized party over a period of three months—remains in the possession of Defendant, is protected from further access and acquisition by unauthorized individuals and breaches, and seeks to remedy the harms he has suffered, and will continue to suffer, on behalf of himself and similarly situated individuals whose Sensitive Information was accessed and acquired by an unauthorized party as a result of Defendant's Data Breach.

29. Plaintiff brings this action to remedy these harms on behalf of himself and all similarly situated individuals whose Sensitive Information was accessed and acquired by an unauthorized party during the Data Breach. Accordingly, Plaintiff, on behalf of himself and Class Members, asserts claims for (1) negligence; (2) negligence *per se*; (3) breach of contracts to which Plaintiff and Class Members are third–party beneficiaries; (4) breach of implied contracts; (5) unjust enrichment; (6) common law unfair competition; (7) declaratory and injunctive relief; (8) violation of the Illinois Consumer Fraud Act; (9) violation of the Illinois Uniform Deceptive Trade Practices Act; and (10) violation of the Missouri Merchandising Practices Act. Plaintiff seeks the following remedies, among others: injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

C. Plaintiff's Experience

30. Plaintiff Daniel Cozza is a resident of the state of Missouri. Plaintiff Cozza received notice from Defendant that it improperly exposed his name and Social Security number to an unknown third party. After receiving the notice, Plaintiff Cozza checked his accounts for any signs

of fraud. Plaintiff Cozza will continue to monitor his financial and other accounts. This is time Plaintiff Cozza otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life, which is now lost forever and cannot be recaptured.

31. Knowing that thieves stole his Sensitive Information, including his Social Security number, and knowing that his Sensitive Information will likely be sold on the dark web, has caused Plaintiff Cozza great anxiety. He is now very concerned about theft of his identity and financial fraud.

32. Plaintiff Cozza suffered actual injury from having his Sensitive Information exposed and stolen as a result of the Data Breach including, but not limited to: (a) damages to and diminution in the value of his Sensitive Information—a form of intangible property in Defendant's possession; (b) loss of his privacy; (c) ongoing, imminent and impending injury arising from the increased risk of fraud and identity theft; and (d) the time and expense of mitigation efforts resulting from the Data Breach.

33. As a result of the Data Breach, Plaintiff Cozza will continue to be at heightened risk for financial fraud, medical fraud, and identity theft, and the attendant damages, for years to come.

34. Plaintiff Cozza has a continuing interest in ensuring his Sensitive Information, which upon information and belief remains in the possession of Defendant, is protected and safeguarded from future data breaches.

D. Defendant Acquires, Collects, Maintains, and Stores Plaintiff's and Class Members' Sensitive Information.

35. Defendant acquires, collects, and stores massive amounts of Sensitive Information in order to provide its services. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Sensitive Information, Defendant assumed legal and equitable

duties, and knew or should have known it was responsible for protecting Plaintiff's and Class Members' Sensitive Information from unauthorized disclosure.

36. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Sensitive Information. Plaintiff and Class Members relied on Defendant to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

E. The Value of Sensitive Information and the Effects of Unauthorized Disclosure.

37. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[9] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[10] That trend continues.

38. Defendant was well aware the Sensitive Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

39. Sensitive Information is a valuable commodity to identity thieves. As the Federal Trade Commission ("FTC") recognizes, Sensitive Information identity thieves can commit an array of crimes including identify theft, medical and financial fraud.[11] Indeed, a robust "cyber

[9] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/post/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout/ (last accessed Dec. 21, 2021).

[10] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review,* available at: *https://www.idtheftcenter.org/wp-content/uploads/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf* (last accessed Dec. 21, 2021).

[11] Federal Trade Commission, *What to Know About Identity Theft*, available at: https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Dec. 21, 2021).

black market" exists where criminals openly post stolen Sensitive Information on multiple underground Internet websites, commonly referred to as the dark web.

40. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now–defunct AlphaBay,

> are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target.[12]

41. Consumers' Sensitive Information remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[13] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[14] Sensitive Information has

[12] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last accessed Dec. 21, 2021).

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Dec. 21, 2021).

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Dec. 21, 2021).

also been valued on the dark web at approximately $1 per line of information.[15] Alternatively, criminals are able to purchase access to entire company data breaches for $900 to $4,500.[16]

42. Individuals also rightfully place a high value not only on their Sensitive Information, but also on the privacy of that data. Researchers have already begun to shed light on how much individuals value their data privacy—and the amount is considerable. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – $44.62."[17] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of Sensitive Information to bad actors—would be exponentially higher today.

43. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

44. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to

[15] https://www.pacetechnical.com/much-identity-worth-black-market/#:~:text=Personally%20identifiable%20information%20is%20sold,at%20a%20fast%20food%20joint (last accessed Dec. 21, 2021).

[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 21, 2021).

[17] Hann, Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Oct. 2002, *available at* https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last accessed Dec. 21, 2021).

apply for more credit in your name. Then, they use the credit cards and do not pay the bills, which damages your credit. You may not find out that someone is using your number until you are turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[18]

45. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' Sensitive Information secure are long lasting and severe. Because many of the data points stolen are persistent—for example, Social Security numbers and names—criminals who purchase the Sensitive Information belonging to Plaintiff and Class Members do not need to use the information to commit fraud immediately. The Sensitive Information can be used or sold for use years later, and as such Plaintiff and Class Members will remain at risk for identity theft indefinitely.

46. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

47. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[19] The Social Security Administration concurs, warning:

---

[18] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Dec. 21, 2021).

[19] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Dec. 21, 2021).

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same . . . .
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[20]

48. Because of this, the information compromised in the Data Breach here is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change. The Sensitive Information compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[21]

49. Once Sensitive Information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional Sensitive Information being harvested from the victim, as well as Sensitive Information from family, friends, and colleagues of the original victim.

---

[20] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Dec. 2013), *available at*: http://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Dec. 21, 2021).

[21] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Dec. 21, 2021).

50. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet–enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[22]

51. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

52. Data breaches facilitate identity theft as hackers obtain consumers' Sensitive Information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' Sensitive Information to others who do the same.

53. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use Sensitive Information to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[23] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states identity theft victims will

[22] FBI, *2019 Internet Crime Report Released, Data Reflects an Evolving Threat and the Importance of Reporting* (Feb. 11, 2020), *available at*: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last accessed Dec. 21, 2021).

[23] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last accessed Dec. 21, 2021).

face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[24]

54. Additionally, the frequency of cyberattacks has increased significantly in recent years.[25] In fact, "Cyberattacks rank as the fastest growing crime in the US, causing catastrophic business disruption. Globally, cybercrime damages are expected to reach US $6 trillion by 2021."[26]

55. Cybersecurity Ventures, a leading researcher on cybersecurity issues,

> expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.[27]

56. As noted in recent reports by Deloitte and Interpol, cyberattacks have greatly increased in the wake of the COVID-19 pandemic.[28]

57. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Sensitive Information and of the foreseeable consequences if its data

---

[24] *Id.*

[25] *See* https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf (last accessed Dec. 21, 2021).

[26] https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency (last accessed Dec. 21, 2021) (citing Cybersecurity Ventures, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016).

[27] Cybercrime Magazine, *Cybercrime To Cost The World $10.5 Trillion Annually By 2020*, Nov. 13, 2020, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 (last accessed Dec. 21, 2021).

[28] Deloitte, *Impact of COVID-19 on Cybersecurity*, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (last accessed Dec. 21, 2021); Interpol, *Cyberthreats are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception*, https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats (last accessed Dec. 21, 2021).

security systems were breached, including the significant costs that would be imposed on Plaintiff and the Class as a result of a breach.

F. Defendant Failed to Comply with FTC Guidelines.

58. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[29]

59. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[30] The guidelines note businesses should protect the personal customer information they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

60. The FTC further recommends companies not maintain Sensitive Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify third-party service providers have implemented reasonable security measures.[31]

---

[29] Federal Trade Commission, *Start With Security*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Dec. 21, 2021).

[30] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Dec. 21, 2021).

[31] FTC, *Start With Security*, *supra* note 29.

61. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

62. Defendant failed to properly implement basic data security practices—including but not limited to maintaining Sensitive Information longer than needed for authorization of a transaction. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to clients' and/or Plaintiff's and Class Members' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

63. Defendant was at all times fully aware of its obligation to protect client's and/or Plaintiff's and Class Members' Sensitive Information because of its position as a business in the financial sector and employer. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. The Health-Related Information Is Particularly Sought After By Hackers.

64. Defendant had knowledge and understood that unprotected or exposed PHI in the care of companies, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize it by unauthorized accessing of it. For example, the healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[32] Indeed, when compromised, healthcare-related data is among the most sensitive and personally consequential.

[32] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, available at:

65. A report focusing on health care related data breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[33] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[34]

66. As a business collecting, maintaining, storing, and using healthcare information, Defendant knew, or should have known, the importance of safeguarding the Sensitive Information entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to protect the Sensitive Information in its possession or to prevent the Data Breach from occurring.

H. Defendant Failed to Comply with Industry Standards to Safeguard Healthcare Related Information.

67. The Department of Health and Human Services' Office for Civil Rights ("DHHS") notes:

---

https://www.idtheftcenter.org/2018-data-breaches/ (last accessed Sept. 21, 2021), also available at: https://webcache.googleusercontent.com/search?q=cache:GdCeEaa4FmoJ:https://www.idtheftcenter.org/2018-data-breaches/%3Fs%3D+&cd=6&hl=en&ct=clnk&gl=us (last accessed Dec. 21, 2021)

[33] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), available at: https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Dec. 21, 2021).

[34] *Id.*

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly sensitive and valuable data.[35]

68. DHHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment, yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Sensitive Information; (b) educating and training employees on how to protect Sensitive Information; and (c) correcting the configuration of software and network devices.

69. Private cybersecurity firms have also promulgated similar best practices for companies with PHI to bolster cybersecurity and protect against the unauthorized disclosure of information.

70. In light of the abundance and availability of information regarding cybersecurity best practices to safeguard PHI, Defendant should have implemented them. These best practices were known, or should have been known by Defendant, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure the Sensitive Information—including the PHI—in its possession.

I. Plaintiff's and Class Members' Sensitive Information Was Also Subject to a Ransomware Attack—a Distinct Form of Data Breach

71. A ransomware attack is a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the owner pays a fee to the perpetrator.

72. Ransomware attacks are considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

---

[35] HIPAA Journal, *Cybersecurity Best Practices for Healthcare Organizations*, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (last accessed Dec. 21, 2021).

> A breach under the HIPAA Rules is defined as, ". . . the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

73. Also, in a ransomware advisory, the Department of Health and Human Services informed entities covered by HIPAA that "when electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information)."[36]

74. Ransomware attacks also constitute data breaches in the traditional sense. For example, in a ransomware attack on the Florida city of Pensacola, and while the City was still recovering from the ransomware attack, hackers released 2GB of data files from the total 32GB of data that they claimed was stolen prior to encrypting the City's network with the maze ransomware. In the statement given to a news outlet, the hackers said, "***This is the fault of mass media who writes that we don't exfiltrate data*** . . . ."[37]

75. Other security experts agree that when a ransomware attack occurs, a data breach does as well, because such an attack represents a loss of control of the data within a network.[38]

---

[36] *See Fact Sheet: Ransomware and HIPAA*, Health and Human Services, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (last accessed Dec. 22, 2021).

[37] *Pensacola Ransomware: Hackers Release 2GB Data as a Proof*, Cisomag (Dec. 27, 2019), https://www.cisomag.com/pensacola-ransomware-hackers-release-2gb-data-as-a-proof/ (emphasis added) (last accessed Dec. 22, 2021).

[38] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last accessed Dec. 22, 2021).

76. Ransomware attacks are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[39]

77. The ransomware attack on Defendant included Plaintiff's and Class Members' Sensitive Information stored on Defendant's computer system. As part of the Defendant's notice to Plaintiff and Class Members about the Data Breach, Defendant stated the breach included encryption of its systems by the unauthorized actor. Therefore, an unauthorized party now possesses Plaintiff's and Class Members' Sensitive Information because, as previously stated, even if Defendant or the unauthorized party claims the exfiltrated data was deleted, "Proof of deletion is not a thing."[40]

J. Plaintiff and Class Members Suffered Damages.

78. The ramifications of Defendant's failure to keep Plaintiff's and the Class's Sensitive Information secure are long lasting and severe. Once Sensitive Information is stolen,

[39] *Supra,* note 36.

[40] *See* Keith Mukai, *ArbiterSports Was Hacked. Don't Use Them Ever Again*, Medium (Aug. 29, 2020), https://medium.com/@kdmukai_64726/arbitersports-was-hacked-dont-use-them-ever-again-fddea92bcd21 (last accessed Dec. 22, 2021)

fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[41]

79. The Sensitive Information belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant, who did not obtain Plaintiff's or Class Members' consent to disclose their Sensitive Information to any other person as required by applicable law and industry standards.

80. The Data Breach was a foreseeable direct and proximate result of Defendant's failure to:

a. properly safeguard and protect Plaintiff's and Class Members' Sensitive Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law;

b. establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Sensitive Information; and

c. protect against reasonably foreseeable threats to the security or integrity of such information.

81. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect Plaintiff's and Class Members' Sensitive Information.

---

[41] 2014 LexisNexis® True Cost of Fraud℠ Study, *Post-Recession Revenue Growth Hampered by Fraud As All Merchants Face Higher Costs*, available at: https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Dec. 21, 2021).

82. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of the Sensitive Information.

83. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take time that they otherwise would have dedicated to other life demands, such as work, leisure, and family, in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

84. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems," and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[42]

85. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. the compromise, publication, theft, and/or unauthorized use of their Sensitive Information;

b. out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. lost opportunity costs and lost wages associated with efforts expended, and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited

[42] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, available at: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed Dec. 21, 2021).

to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. the current and ongoing risk to their Sensitive Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Sensitive Information;

e. current and future costs in terms of time, effort, and money that will be expended to prevent, mitigate, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of Plaintiff's and Class Members' lives; and

f. stress, anxiety, and other related forms of emotional distress.

86. In addition to a remedy for these harms, Plaintiff and the Class Members maintain an undeniable interest in ensuring their Sensitive Information is secure, remains secure, and is not subject to further misappropriation and/or theft.

K. Defendant's Delay in Identifying and Reporting the Breach Caused Additional Harm.

87. It is axiomatic that:

> The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[43]

88. Indeed, once a data breach has occurred:

[43] Business Wire¸ *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, available at: https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million (last accessed Dec. 21, 2021).

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills, insurance invoices, and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves (internal citations omitted).[44]

89. Although their Sensitive Information was improperly exposed, viewed, and stolen beginning on or about August 20, 2020, through December 1, 2020, affected persons were not notified of the Data Breach until, at the earliest, November 30, 2021, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

90. As a result of Defendant's delay in detecting and notifying client's and/or Plaintiff's and Class Members' of the Data Breach, Plaintiff's and Class Members' risk of fraud has been driven even higher.

V. CLASS ALLEGATIONS

91. Plaintiff seeks relief on behalf of himself and as representatives of all others similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and (c)(4), Plaintiff seeks certification of a Nationwide class, defined as follows:

> All persons residing in the United States whose Sensitive Information was accessed and acquired by an unauthorized party in the Data Breach announced by Defendant in or about November 30, 2021 (the "Nationwide Class").

92. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims under the laws of the individual States, and on behalf of separate statewide classes, defined as follows:

---

[44] Consumer Reports, *The Data Breach Next Door Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too*, January 31, 2019, available at: https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last accessed Dec. 21, 2021).

> **Missouri Subclass:** All persons residing in the state of Missouri whose Sensitive Information was accessed and acquired by an unauthorized party in the Data Breach announced by Defendant in or about November 30, 2021 (the "Missouri Class").

93. Where appropriate, the Nationwide Class and Statewide Classes are collectively referred to as the "Class."

94. Excluded from the Class are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the Judge(s) and Court personnel in this case and any members of their immediate families.

95. Plaintiff reserves the right to amend the class definitions, including creating additional subclasses as necessary, after having had an opportunity to conduct discovery.

96. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

97. All Class Members are readily ascertainable in that Defendant has access to addresses and other contact information for all Class Members, which can be used for providing notice to Class Members.

98. **Numerosity.** Consistent with Fed. R. Civ. P. 23(a)(1), the class members are so numerous and geographically dispersed that joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiff at this time, the proposed Class includes approximately 274,15 individuals whose Sensitive Information was compromised in the Data Breach. Class Members may be identified through objective means. Class Members may be

notified of the pendency of this action by recognized, Court–approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

99. **Commonality and Predominance.** Consistent with Fed. R. Civ. P. 23(a)(2) and 23(b)(3), this action involves common questions of law and fact predominating over any questions that may affect only individual Class Members. Common questions include:

a. Whether Defendant had a duty to protect the Sensitive Information in its possession;

b. Whether Defendant's allowing Plaintiff's and Class Members' Sensitive Information to be accessed, viewed, and/or obtained by unauthorized persons without prior written authorization from Plaintiff or Class Members was permissible;

c. Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

d. Whether Defendant engaged in the wrongful conduct alleged in this Complaint;

e. Whether Defendant's conduct was unfair, unconscionable, and/or unlawful;

f. Whether Defendant failed to implement and maintain industry standard, adequate, and reasonable systems and security procedures and practices to protect Plaintiff's and Class Members' Sensitive Information;

g. Whether Defendant was negligent in failing to implement industry standard, adequate, and reasonable security procedures and practices;

h. Whether Defendant was negligent in failing to discover continuing unauthorized access to its network for a period of approximately three months—between August 20, 2020, and December 1, 2020;

i. Whether Defendant's failure to implement industry standard, adequate, and reasonable data security measures allowed the breach to occur;

j. Whether Defendant owed a duty to Plaintiff and Class Members to adequately protect their Sensitive Information, and to provide timely notice of the Data Breach to Plaintiff and Class Members;

k. Whether Defendant breached its duties to protect Plaintiff's and Class Members' Sensitive Information by failing to provide industry standard, adequate, and reasonable data security, and failing to provide appropriate and timely notice of the Data Breach to Plaintiff and Class Members;

l. Whether Defendant failed to exercise reasonable care in the hiring, training, and/or supervision of its employees and agents;

m. Whether Defendant's conduct constituted deceptive trade practices;

n. Whether Defendant's conduct constituted unfair and deceptive acts and practices;

o. Whether Plaintiff and Class Members are third–party beneficiaries to the contracts between Defendant and its clients;

p. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Plaintiff's and Class Members' Sensitive Information;

q. Whether Defendant adequately addressed and fixed the vulnerabilities permitting the Data Breach to occur;

r. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Defendant's failure to reasonably and/or adequately protect its network;

s. Whether Plaintiff and Class Members are entitled to recover damages; and

t. Whether Plaintiff and Class Members are entitled to declaratory relief and equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

100. **Typicality.** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of the claims of other Class Members in that Plaintiff, like all Class Members, had his Sensitive Information compromised, breached, and stolen in the Data Breach. Plaintiff's damages and injuries are akin to other Class members, and Plaintiff asserts the same claims and forms of relief as the Class.

101. **Adequacy.** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff is a member of the Class defined herein; is committed to vigorously pursuing this matter against Defendant to obtain relief for the Class; and has no interests that are antagonistic to, or in conflict with, the interests of other Class Members. Plaintiff retained counsel who are competent and experienced in litigating class actions and complex litigation, including privacy litigation of this kind. Plaintiff and his counsel intend to vigorously prosecute this case, and will fairly and adequately protect the Class's interests.

102. **Superiority.** Consistent with Fed. R. Civ. P. 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment

of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their individual claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members were harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of inconsistent outcomes of individual actions, and repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff is unaware of any difficulties that might be encountered in this litigation that would preclude its maintenance as a class action.

103. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the common questions of law and fact predominate over any questions affecting individual Class Members, a class action is superior to other available methods for the fair and efficient adjudication of this controversy, and the requirements of Rule 23(a) are met.

104. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because Defendant, through its uniform conduct, acted or failed and refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Defendant continues to maintain its inadequate security practices, retain possession of Plaintiff's and Class Members' Sensitive Information, and has not been forced to change its practices or relinquish Sensitive Information by nature of other civil suits or government enforcement actions, thus making injunctive relief a live issue and appropriate to the Class as a whole.

105. Likewise, particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present particular, common issues, the resolution of which would

materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Plaintiff's and Class Members' Sensitive Information was accessed and/or acquired by an unauthorized party in the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and Class Members;

c. Whether Defendant failed to take adequate and reasonable steps to safeguard Plaintiff's and Class Members' Sensitive Information;

d. Whether Defendant failed to adequately monitor its data security systems;

e. Whether Defendant failed to comply with applicable laws, regulations, and/or industry standards relating to data security amounting to negligence;

f. Whether Defendant's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

g. Whether Defendant knew or should have known that it did not employ adequate and reasonable measures to keep Plaintiff's and Class Members' Sensitive Information secure; and

h. Whether Defendant's failure to adhere to FTC data security obligations, industry standards, and/or measures recommended by data security experts caused the Data Breach.

VI. CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff, the Nationwide Class and Missouri Subclass)

106. Plaintiff incorporates paragraphs 1 through 105 as though fully set forth herein.

107. Defendant collected, maintained, analyzed, and used Plaintiff's and Class Members' Sensitive Information, and by doing so undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard their Sensitive Information, and to use industry standard, commercially available, and reasonable methods to do so. At all times, Defendant knew Plaintiff's and Class Members' Sensitive Information was private and confidential, was required to be kept private and confidential, and the types of harm Plaintiff and Class Members could and would suffer if the Sensitive Information was wrongfully disclosed.

108. Defendant owed a duty of care not to subject Plaintiff and Class Members, along with their Sensitive Information, to an unreasonable risk of harm because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices by Defendant.

109. Because of its duty of care to prevent foreseeable harm to Plaintiff and Class Members, and Defendant therefore had, and still has, a duty to take adequate and reasonable steps to safeguard their Sensitive Information from unauthorized access and/or acquisition (theft). More specifically, this duty includes:

a. Exercising reasonable care in the hiring, training, and/or supervising of its employees and agents entrusted with access to and safeguarding of Plaintiff's and Class Members' Sensitive Information on cyber security measures and industry standards regarding the safety and safeguarding of Sensitive Information;

b. Designing, maintaining, and testing Defendant's data security systems, data storage architecture, and data security protocols to ensure Plaintiff's and Class Members' Sensitive Information in Defendant's possession was and

is adequately secured and protected from unauthorized access and/or acquisition;

c. Implementing processes to timely and adequately detect an unauthorized breach of Defendant's security systems and data storage architecture;

d. Timely acting on all suspicions, warnings, and alerts, including public information, regarding Defendant's security vulnerabilities and potential compromise of Plaintiff's and Class Members' Sensitive Information in its possession; and

e. Maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements.

110. Defendant had a common law duty to prevent foreseeable harm to Plaintiff and Class Members. The duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices of Defendant in its affirmative collecting, maintaining, analyzing, and using of Plaintiff's and Class Members' Sensitive Information. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by Defendant's failure to protect their Sensitive Information because unauthorized parties, hackers, and other malicious actors routinely attempt to access and steal such information for use in nefarious purposes, but Defendant also knew it was more likely than not that Plaintiff and Class Members would be harmed as a result.

111. Defendant knew, or should have known, of the risks inherent in collecting, maintaining, analyzing, and using Sensitive Information, the vulnerabilities of its data security systems, and the importance of adequate and industry standard security. Defendant knew or should have known about numerous, well-publicized data breaches and of industry security warnings.

112. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' Sensitive Information.

113. Defendant's duties to use adequate and reasonable security measures also arose as a result of the special relationship existing between it, on the one hand, and Plaintiff and Class Members, on the other hand. This special relationship, recognized in laws and regulations, arose because Defendant collected, maintained, analyzed, and used Plaintiff's and Class Members' Sensitive Information in order to perform its services. Defendant alone had the duty to and could have ensured its security system and data storage architecture was sufficient to prevent or minimize the Data Breach.

114. Further, the policy of preventing future harm weighs in favor of finding a special relationship between Defendant on the one hand, and Plaintiff and Class Members on the other. If companies are not held accountable for failing to implement minimum industry-standard security practices and procedures to safeguard Sensitive Information in their possession, companies will have no incentive to—and ultimately will not—take the necessary steps to protect against future security breaches.

115. Defendant also owed a duty to timely disclose the material fact that its computer network and data security practices and protocols were inadequate to safeguard Plaintiff's and Class Members' Sensitive Information from unauthorized access and acquisition.

116. Defendant also had independent duties under state and federal laws requiring it to reasonably safeguard Plaintiff's and Class Members' Sensitive Information, and promptly notify them about the data breach.

117. Defendant solicited, gathered, analyzed, stored, and used Plaintiff's and Class Members' Sensitive Information to provide its services—which affects commerce.

118. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, and/or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Sensitive Information. Defendant also breached its duty to Plaintiff and Class Members to adequately protect and safeguard Sensitive Information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to and acquisition of unsecured Sensitive Information. Defendant breached these duties through the conduct alleged in this Complaint by, including without limitation:

a. Failing to protect the Sensitive Information in its possession;

b. Failing to implement the minimum industry–standard security practices and procedures;

c. Failing to maintain adequate computer systems and data security practices to safeguard the Sensitive Information in its possession despite knowing its vulnerabilities;

d. Allowing unauthorized access to and acquisition of Plaintiff's and Class Members' Sensitive Information;

e. Failing to implement adequate system and event monitoring;

f. Failing to disclose the material fact that its computer systems and data security practices were inadequate to safeguard the Sensitive Information in its possession from unauthorized access and acquisition; and

g. Failing to disclose the material fact of the Data Breach to Plaintiff and Class Members in a timely and accurate manner.

119. Furthering Defendant's negligent practices, Defendant also breached its duties by failing to implement adequate security supervision and oversight of the Sensitive Information with which it was and is entrusted—in spite of the known risk and foreseeable likelihood of breach and misuse—that permitted an unauthorized party to access and acquire Plaintiff's and Class Members' Sensitive Information, and intentionally disclose the Sensitive Information to an unauthorized party without prior consent.

120. The injuries suffered by Plaintiff and Class Members were proximately and directly caused by Defendant's breach of its duties—specifically its failure to exercise adequate and reasonable care in hiring, training, and/or supervising its employees and agents tasked with safeguarding and/or with access to Plaintiff's and Class Members' Sensitive Information, failure to monitor and/or test its data security system, and failure to monitor or otherwise follow reasonable industry standard security measures to protect Plaintiff's and Class Members' Sensitive Information.

121. When individuals—such as Plaintiff and Class Members—have their personal information stolen, they are placed at current and ongoing risk of identity theft, and need to take steps to protect themselves, including, for example, paying for credit monitoring services, and purchasing or obtaining credit reports to protect themselves from identity theft. The credit monitoring services and purchasing or obtaining credit reports are required because of the present economic risk and harm—unauthorized parties exfiltrated Sensitive Information enabling them to commit identity theft, and secure fraudulent loans, leases, and credit cards. And, the unauthorized parties are likely to continue attempting their identity theft and fraudulent activities for the foreseeable future, so Plaintiff and Class Members have been injured and are exposed to a real risk of misuse of their Sensitive Information.

122. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Sensitive Information would not have been accessed and acquired by an unauthorized party. And as a direct and proximate result of Defendant's failure to exercise adequate and reasonable care and use industry standard, commercially available, adequate, and reasonable security measures, Plaintiff's and Class Members' Sensitive Information was accessed and acquired by an unauthorized party who could—and likely will—use the information to commit identity or financial fraud. Plaintiff and Class Members face the ongoing concrete, imminent, and impending substantially heightened risk of identity theft, fraud, and misuse of their Sensitive Information.

123. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect Plaintiff's and Class Members' Sensitive Information, and the harm suffered and/or risk of imminent harm suffered by Plaintiff and Class Members.

124. It was foreseeable Defendant's failure to exercise reasonable care to safeguard the Sensitive Information in its possession and/or control would lead to one or more types of injury to Plaintiff and Class Members. And the Data Breach was foreseeable given the known, publicized, high frequency of cyberattacks and data breaches against companies accessing, maintaining, storing, and/or utilizing Sensitive Information.

125. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of, or should have known of, the inherent risks in collecting and storing Sensitive Information, the critical importance of providing adequate security for Sensitive Information, the current cyber scams being perpetrated using Sensitive Information, and its own inadequate security practices, procedures, and protocols in place to secure Plaintiff's and Class Members' Sensitive Information.

126. Plaintiff and Class Members have no ability to protect their Sensitive Information in Defendant's possession.

127. Defendant alone was in a position to protect against the harm and injuries suffered by Plaintiff and Class Members as a result of the Data Breach.

128. As a direct and proximate result of Defendant's conduct and violations of the above–mentioned statutes, Plaintiff and Class Members have suffered, and continue to suffer, damages arising from the Data Breach as described herein, and are entitled to compensatory, consequential, nominal, and punitive damages in an amount to be proven at trial. Such injuries and damages include but are not limited to those described above, including:

a. Actual identity theft and current and ongoing risk of identity fraud;

b. Loss of the opportunity to control how their Sensitive Information is used;

c. The compromise, publication, and/or theft of their Sensitive Information;

d. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information;

e. Lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports;

f. The current and ongoing risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Sensitive Information in Defendant's continued possession;

g. Future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information accessed and acquired as a result of the Data Breach—which may take months if not years to discover, detect, and remedy;

h. Future out-of-pocket expenses associated with paying for fraudulent charges resulting from identity theft, and/or unauthorized use of their Sensitive Information;

i. The diminished value of their Sensitive Information;

j. Other economic harm;

k. Emotional distress; and

l. The necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

129. The nature of other forms of damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft of the Sensitive Information during the Data Breach mentioned above.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Nationwide Class and Missouri Subclass)

130. Plaintiff incorporates paragraphs 1 through 105 as though fully set forth herein.

131. Defendant had duties to safeguard Plaintiff's and Class Members' Sensitive Information that arose through certain statutes and regulations.

132. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Sensitive Information. Similar state–specific statutory causes of action—such as consumer fraud and unfair trade practices acts—provide for such a duty, as well.

133. Plaintiff and Class Members are members of the classes of persons the foregoing statute is intended to protect.

134. The essential purpose of the statute is to protect from the same or similar kind of harm caused to Plaintiff and Class Members, as a direct and proximate result of Defendant's breach of those statutory and regulatory duties.

135. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Sensitive Information.

136. Defendant's breach of its duties arising out of the foregoing statute constitutes negligence *per se*.

137. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' Sensitive Information would not have been compromised and they would not have been harmed.

138. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class

Members to experience the foreseeable harms associated with the exposure and exfiltration of their Sensitive Information, including increased risk of identity theft.

139. As a direct and proximate result of Defendant's violation of the foregoing statutes and regulations, Plaintiff and Class Members were injured as described in detail herein, and are entitled to compensatory, consequential, nominal, and punitive damages in an amount to be proven at trial. Such injuries and damages include but are not limited to those described above, including:

a. Actual identity theft and current and ongoing risk of identity fraud;

b. Loss of the opportunity to control how their Sensitive Information is used;

c. The compromise, publication, and/or theft of their Sensitive Information;

d. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information;

e. Lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports;

f. The current and ongoing risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures

to protect Plaintiff's and Class Members' Sensitive Information in Defendant's continued possession;

g. Future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information accessed and acquired as a result of the Data Breach—which may take months if not years to discover, detect, and remedy;

h. Future out-of-pocket expenses associated with paying for fraudulent charges resulting from identity theft, and/or unauthorized use of their Sensitive Information;

i. The diminished value of their Sensitive Information;

j. Other economic harm;

k. Emotional distress; and

l. The necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

140. The nature of other forms of damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft of the Sensitive Information during the Data Breach mentioned above.

COUNT III
Breach of Contracts to Which Plaintiff and Class Members Are Third–Party Beneficiaries
(On Behalf of Plaintiff and the Nationwide Class and Missouri Subclass)

141. Plaintiff incorporates paragraphs 1 through 105 as though fully set forth herein.

142. At all times relevant, Defendant had express or implied contracts or agreements with clients to provide services.

143. Plaintiff and Class Members are intended third–party beneficiaries of contracts entered into between Defendant and its clients because Plaintiff's and Class Members' Sensitive Information is the subject matter of the contracts and for which Defendant agreed to provide its services.

144. As previously alleged, Defendant breached these contracts by failing to employ adequate and industry standard information security practices to secure Plaintiff's and Class Members' Sensitive Information, resulting in the Data Breach and the theft and foreseeable misuse of Plaintiff and Class Members' Sensitive Information by unauthorized third persons.

145. Plaintiff and Class Members have a right to recovery for breach because one or more of the parties to these contracts intended to give Plaintiff and Class Members benefits related to the performance promised in the contracts.

146. As a direct and proximate result of Defendant's breaches of these contracts, Plaintiff and Class Members have suffered, and continue to suffer, injuries and damages arising from the Data Breach as alleged above.

147. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft of the Sensitive Information during the Data Breach mentioned above.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class and Missouri Subclass)

148. Plaintiff incorporates paragraphs 1 through 105 as though fully set forth herein.

149. Defendant offered accounting, tax, consulting, payroll, and assurance solutions services to client and/or Plaintiff and Class Members in exchange for compensation.

150. Plaintiff's and Class Members' Sensitive Information, including their full name, Social Security number, and other private and sensitive information, was provided Defendant in order to receive Defendant's services.

151. Plaintiff and Class Members paid money, or on information and belief, money was paid on their behalf, to Defendant in exchange for services, along with Defendant's promise to protect their Sensitive Information, from unauthorized disclosure. These exchanges constituted an agreement between the parties.

152. Defendant, as a certified public accounting firm, promised to comply with relevant laws and to protect Plaintiff's and Class Members' Sensitive Information.

153. Implicit in the agreement between Plaintiff and Class Members or others on their behalf, and Defendant regarding the Sensitive Information was Defendant's obligation to: (a) use such Sensitive Information for business purposes only; (b) take reasonable and adequate steps to safeguard that Sensitive Information; (c) prevent unauthorized disclosures of the Sensitive Information; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information; (e) reasonably safeguard and protect Plaintiff's and Class Members' Sensitive Information from unauthorized disclosure or uses; and (f) retain the Sensitive Information only under conditions that kept such information secure and confidential.

154. Without such implied contracts, Plaintiff and Class Members would not have provided their Sensitive Information to Defendant or allowed it to be provided to Defendant on their behalf.

155. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant. Defendant was therefore required to reasonably safeguard and protect

Plaintiff's and Class Members' Sensitive Information from unauthorized disclosure and/or use. However, Defendant did not.

156. Defendant breached the implied contracts with Plaintiff and Class Members by failing to (a) reasonably safeguard and protect Plaintiff's and Class Members' Sensitive Information, which was compromised as a result of the Data Breach; and (b) comply with its promise to abide by applicable laws.

157. Defendant's failure to implement adequate measures to protect Plaintiff's and Class Members' Sensitive Information violated the purpose of the agreement between the parties: Plaintiff's and Class Members' payment, and/or payment made on their behalf, in exchange for Defendant's services.

158. Defendant was on notice that its systems and data security protocols could be inadequate, yet failed to invest in the proper safeguarding of Plaintiff's and Class Members' Sensitive Information.

159. Instead of spending adequate financial resources to safeguard Plaintiff's and Class Members' Sensitive Information, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiff and Class Members.

160. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to:

a. Actual identity theft and current and ongoing risk of identity fraud;

b. Loss of the opportunity to control how their Sensitive Information is used;

c. The compromise, publication, and/or theft of their Sensitive Information;

d. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information;

e. Lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports;

f. The current and ongoing risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Sensitive Information in Defendant's continued possession;

g. Future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information accessed and acquired as a result of the Data Breach—which may take months if not years to discover, detect, and remedy;

h. Future out-of-pocket expenses associated with paying for fraudulent charges resulting from identity theft, and/or unauthorized use of their Sensitive Information;

i. The diminished value of their Sensitive Information;

j. Other economic harm;

k. Emotional distress; and

l. The necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class and Missouri Subclass)

161. Plaintiff incorporates paragraphs 1 through 105 as though fully set forth herein.

162. Plaintiff and Class Members conferred a monetary benefit on Defendant, either directly or indirectly. Specifically, they purchased goods and services, or on information and belief they were purchased on Plaintiff's and Class Members' behalf, from Defendant and in so doing Defendant was provided with their Sensitive Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Sensitive Information protected with adequate data security.

163. Defendant knew Plaintiff and Class Members conferred a benefit that Defendant accepted. Defendant profited from these transactions and used Plaintiff's and Class Members' Sensitive Information for business purposes.

164. The amounts Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

165. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

166. Defendant failed to secure Plaintiff's and Class Members' Sensitive Information and, therefore, Defendant did not provide full compensation for the benefit provided by Plaintiff and Class Members.

167. Defendant acquired the Sensitive Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

168. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Sensitive Information, they would have taken measures to make sure Defendant did not receive their Sensitive information.

169. Plaintiff and Class Members have no adequate remedy at law.

170. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. Actual identity theft and current and ongoing risk of identity fraud;

b. Loss of the opportunity to control how their Sensitive Information is used;

c. The compromise, publication, and/or theft of their Sensitive Information;

d. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information;

e. Lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely

reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports;

f. The current and ongoing risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Sensitive Information in Defendant's continued possession;

g. Future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information accessed and acquired as a result of the Data Breach—which may take months if not years to discover, detect, and remedy;

h. Future out-of-pocket expenses associated with paying for fraudulent charges resulting from identity theft, and/or unauthorized use of their Sensitive Information;

i. The diminished value of their Sensitive Information;

j. Other economic harm;

k. Emotional distress; and

l. The necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

COUNT VI
Common Law Unfair Competition
(On Behalf of Plaintiff, and the Nationwide Class and Missouri Subclass)

171. Plaintiff incorporates paragraphs 1 through 105 as though fully set forth herein.

172. Defendant's acts described herein constitute unfair competition in violation of the common law of the State of Illinois.

173. Defendant's acts constituting unfair competition in violation of the common law of the State of Illinois are willful acts, done with full knowledge of Plaintiff's and Class Member's rights.

174. Defendant's acts, and described herein, have caused direct and proximate damage to Plaintiff and Class Members. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendant's unfair competition practices. Plaintiff's and Class Members' Sensitive Information was taken and is in the hands of those who will use it for their own advantage, and/or is being sold for value, making it clear that the stolen information is of tangible value. Plaintiff and Class Members also will suffer and/or have suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

175. Defendant's actions described herein have caused, and will continue to cause, Plaintiff and Class Members to suffer irreparable harm unless enjoined and/or restrained by this Court. Plaintiff and Class Members have no adequate remedy at law and is thus damaged in an amount not yet determined.

COUNT VII
Declaratory and Injunctive Relief
(On Behalf of Plaintiff and the Nationwide Class and Missouri Subclass)

176. Plaintiff incorporates paragraphs 1 through 105 as though fully set forth herein.

177. Plaintiff brings this cause of action under the federal Declaratory Judgment Act, 28 U.S.C. § 2201.

178. As previously alleged, Plaintiff and Class Members entered into an express and/or implied contract requiring Defendant to provide adequate security for the Sensitive Information it collected regarding Plaintiff and Class Members.

179. Defendant owes a duty of care to Plaintiff and Class Members, requiring Defendant to adequately secure Plaintiff's and Class Members' Sensitive Information.

180. Defendant still possess Plaintiff's and Class Members' Sensitive Information.

181. Since the Data Breach, Defendant has announced few if any changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices that permitted the Data Breach to occur and, thereby, prevent future data breaches.

182. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the Sensitive Information in Defendant's possession is even more vulnerable to cyberattack.

183. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff's and Class Members' Sensitive Information. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their Sensitive Information and Defendant's failure to address the security failings that led to such exposure.

184. There is no reason to believe Defendant's security measures are any more adequate to meet its contractual obligations and legal duties now than they were before the Data Breach.

185. Plaintiff, therefore, seeks a declaration that (1) Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to ordering Defendant:

a. engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. engage third-party security auditors and internal personnel to run automated security monitoring;

c. audit, test, and train its security personnel regarding any new or modified procedures;

d. segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. purge, delete, and destroy in a reasonably secure manner Sensitive Information not necessary for its provisions of services;

f. conduct regular computer system scanning and security checks;

g. routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. to meaningfully educate its current, former, and prospective clients and Class Members about the threats they face as a result of the loss of their Sensitive Information to third parties, as well as the steps they must take to protect themselves.

COUNT VIII
Violation of the Illinois Consumer Fraud Act, 815 ILCS §§ 505, *et seq.*
(On Behalf of the Plaintiff, and the National Class)

186. Plaintiff incorporates paragraphs 1 through 105 as though fully set forth herein

187. This claim is brought under the laws of Illinois and on behalf of all other natural persons whose Sensitive Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

188. Defendant is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

189. Plaintiff and Class Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

190. Defendant's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

191. Defendant's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members' Sensitive Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Sensitive Information, including duties imposed by the FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill.

Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class Members' Sensitive Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Sensitive Information, including duties imposed by the FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Failing to timely and adequately notify clients, Plaintiff, and Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' Sensitive Information;

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Sensitive Information, including duties imposed by FCRA, FTC Act, Illinois laws regulating the use and

disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a); and

i. By failing to provide disclose the Data Breach in a timely fashion, in violation of 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*

192. Defendant's representations and omissions were material because they were likely to deceive reasonable clients and consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Sensitive Information.

193. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Class Members, into believing that their clients' or their Sensitive Information would not be exposed to unauthorized parties.

194. Defendant intended to mislead its customers, Plaintiff, and Class Members, and induce them to rely on its misrepresentations and omissions.

195. The above unfair and deceptive practices and acts by Defendant offend public policy. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

196. Defendant acted intentionally and knowingly to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff's and Class Members' rights.

197. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including, but not limited to:

a. Actual identity theft and current and ongoing risk of identity fraud;

b. Loss of the opportunity to control how their Sensitive Information is used;

c. The compromise, publication, and/or theft of their Sensitive Information;

d. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information;

e. Lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports;

f. The current and ongoing risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Sensitive Information in Defendant's continued possession;

g. Future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information accessed and acquired as a result of the Data Breach—which may take months if not years to discover, detect, and remedy;

h. Future out-of-pocket expenses associated with paying for fraudulent charges resulting from identity theft, and/or unauthorized use of their Sensitive Information;

i. The diminished value of their Sensitive Information;

j. Other economic harm;

k. Emotional distress; and

l. The necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

198. Plaintiff and Class Members seek all monetary and non–monetary relief allowed by law, including damages, restitution, nominal and punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT IX
Violation of the Illinois Uniform Deceptive Trade Practices Act,
815 ILCS §§ 510/2, *et seq.*
(On Behalf of Plaintiff and the National Class)

199. Plaintiff incorporates paragraphs 1 through 105 as though fully set forth herein.

200. This claim is brought under the laws of Illinois and on behalf of all other natural persons whose Sensitive Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

201. Defendant is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

202. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

203. Defendant's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Sensitive Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Sensitive Information, including duties imposed by FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Sensitive Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Sensitive Information, including duties imposed by the FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Failing to timely and adequately notify Plaintiff and Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' Sensitive Information;

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Sensitive Information, including duties imposed by the FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

204. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of Plaintiff's and Class Members' Sensitive Information.

205. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Class Members, into believing that their Sensitive Information would not be exposed to unauthorized parties.

206. The above unfair and deceptive practices and acts by Defendant offend and violate public policy. These acts caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

207. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive trade practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non–monetary damages, including, but not limited to:

a. Actual identity theft and current and ongoing risk of identity fraud;

b. Loss of the opportunity to control how their Sensitive Information is used;

c. The compromise, publication, and/or theft of their Sensitive Information;

d. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information;

e. Lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent

researching how to prevent, detect, contest, and recover from identity theft, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports;

f. The current and ongoing risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Sensitive Information in Defendant's continued possession;

g. Future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information accessed and acquired as a result of the Data Breach—which may take months if not years to discover, detect, and remedy;

h. Future out-of-pocket expenses associated with paying for fraudulent charges resulting from identity theft, and/or unauthorized use of their Sensitive Information;

i. The diminished value of their Sensitive Information;

j. Other economic harm;

k. Emotional distress; and

l. The necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

208. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

COUNT X
Missouri Merchandising Practices Act, Mo. Stat. § 407.010, *et seq.*
(On Behalf of Plaintiff and the Missouri Subclass)

209. Plaintiff incorporates paragraphs 1 through 105 as though fully set forth herein.

210. Defendant engaged in unlawful, unfair, and deceptive acts and practices, with respect to the sale and advertisement of the services in violation of Mo. Stat. § 407.020(1), including by representing that Defendant would adequately protect Plaintiff's and Missouri Class members' Sensitive Information from unauthorized disclosure and release, and comply with relevant state and federal privacy laws. These injuries outweigh any benefits to consumers or to competition.

211. The above unfair and deceptive practices and acts by Defendant violate and offend public policy, and have caused, and will continue to cause substantial injury to Plaintiff and Class Members.

212. Defendant knew or should have known that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' Sensitive Information.

213. Defendant's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Missouri Class.

214. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiff and the Missouri Class suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their personal information.

215. Plaintiff and Missouri Class members seek relief under Mo. Stat. § 407.025, including, but not limited to injunctive relief, actual damages, nominal damages, punitive damages, and attorneys' fees and costs.

VII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class(es) proposed in this Complaint, respectfully requests the Court enter judgment in his favor and against Defendant as follows:

a. For an Order certifying the Class(es), as defined herein, and appointing Plaintiff and his Counsel to represent the Nationwide Class, or in the alternative the separate Missouri SubClass;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the Data Breach and access and acquisition of Plaintiff's and Class Members' Sensitive Information by an unauthorized party, and from failing to issue prompt disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to use appropriate cyber security methods and policies with respect to Sensitive Information collection, storage, maintenance, analysis, use, and protection;

d. A mandatory injunction directing Defendant to adequately safeguard Plaintiff's and Class Members' Sensitive Information by implementing improved security procedures and measures; specifically:

i. Requiring Defendant to protect, including through encryption, all data collected, maintained, and analyzed through the course of its

business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

ii. Requiring Defendant to delete, destroy, and purge the Sensitive Information of Plaintiff and the Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class Members;

iii. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Sensitive Information;

iv. Prohibiting Defendant from maintaining Plaintiff's and Class Members' Sensitive Information on a cloud-based database;

v. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. Requiring Defendant to conduct regular database scanning and security checks;

x. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Sensitive Information, as well as protecting Plaintiff's and Class Members' Sensitive Information;

xi. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. Requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with

Defendant's policies, programs, and systems for protecting Sensitive Information;

xiii. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. Requiring Defendant to meaningfully educate all Class Members about the threats they face as a result of the loss of their confidential Sensitive Information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

xvi. For a period of 10 years, appointing a qualified and independent third-party assessor to conduct a System and Organization Controls ("SOC") 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xvii. Requiring Defendant to design, maintain, and test its computer systems to ensure Sensitive Information in its possession is adequately secured and protected;

xviii. Requiring Defendant to disclose any future data breaches in a timely and accurate manner;

xix. Requiring Defendant to implement multi–factor authentication requirements;

xx. Requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxi. Requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class Members.

e. An award of other declaratory, injunctive, and equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

f. An award of restitution; compensatory, consequential, and general damages to Plaintiff and Class Members, including nominal damages as allowed by law in an amount to be determined at trial or by this Court;

g. An award of actual or statutory damages to Plaintiff and Class Members in an amount to be determined at trial or by this Court;

h. An award of reasonable litigation expenses and costs and attorneys' fees to the extent allowed by law;

i. An award of pre– and post–judgment interest to Plaintiff and Class Members, to the extent allowable; and

j. Award such other and further relief as equity and this Court may deem just and proper.

VIII. JURY TRIAL DEMANDED

Plaintiff requests a trial by jury on all issues so triable.

NOTICE TO THE ILLINOIS ATTORNEY GENERAL

A copy of this Complaint will be mailed to the Illinois Attorney General.

Dated: December 22, 2021

Respectfully submitted,

LOCKRIDGE GRINDAL NAUEN P.L.L.P.

s/Kyle J. Pozan
Karen Hanson Riebel (*pro hac vice forthcoming*)
Kate M. Baxter-Kauf (*pro hac vice forthcoming*)
Kyle Pozan (IL Bar No. 6306761)
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: 612.339.6900
Facsimile: 612.339.0981
kjpozan@locklaw.com
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Gayle M. Blatt (*pro hac vice forthcoming*)
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: 619.238.1811
Facsimile: 619.544.9232
gmb@cglaw.com

Attorneys for Plaintiff and the Class